Módulo III
Ciberseguridad

MARIBEL RODRIGUEZ MARQUEZ

1

Definiciones

A continuación veremos algunas definiciones de Ciberseguridad, seguridad de la información

CIBERSEGURIDAD INTERNACIONAL

Norma ISO/IEC 27032:2012

Preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.

Agencia Europea para la seguridad de la información y las redes

Son todos los aspectos de prevención, previsión, tolerancia, detección, mitigación, eliminación, análisis e investigación de incidentes cibernéticos.

CIBERSEGURIDAD PARA EL GOBIERNO COLOMBIANO

Conpes 3854 de 2016

Conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, tecnologías buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio.

Seguridad de la información

CONFIDENCIALIDAD

Asegurar que solo quien este autorizado tenga acceso a la información

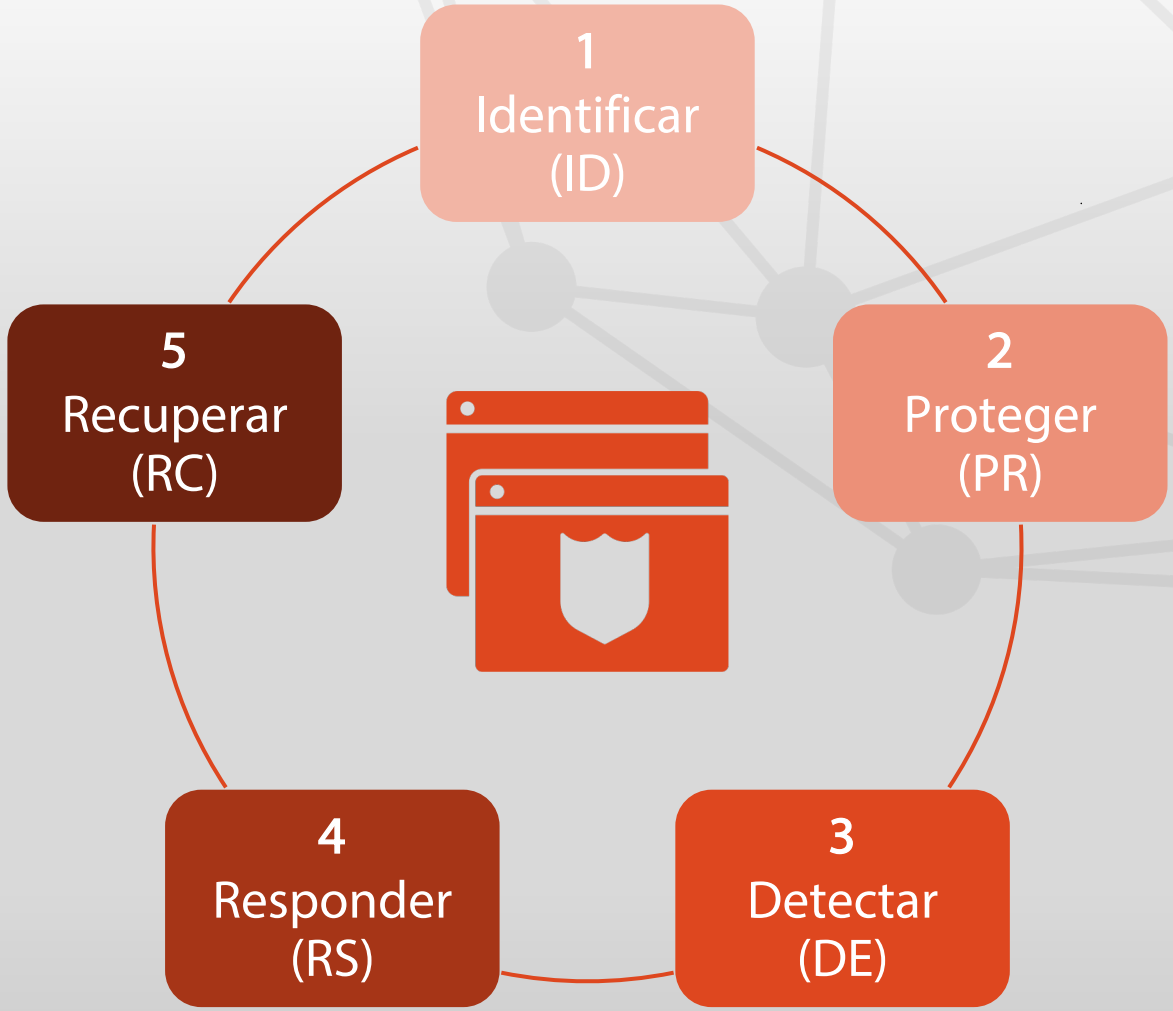
INTEGRIDAD

Proteger la exactitud y estado completo de la información y los métodos de procesamiento

DISPONIBILIDAD

Garantizar que el usuario autorizado tenga acceso a la información en el momento en que lo requiera

Marco de ciberseguridad NIST



¿Qué es un documento CONPES?

El **Consejo Nacional de Política Económica y Social** — CONPES — fue creado por la Ley 19 de 1958. Ésta es la máxima autoridad nacional de planeación y se desempeña como **organismo asesor del Gobierno** en todos los aspectos relacionados con el **desarrollo económico y social del país.**

2011

Documento CONPES 3701.

Lineamientos de política para ciberseguridad y ciberdefensa

2012

Ley 1581

Disposiciones para la protección de datos personales.

2016

Documento CONPES 3854

Política Nacional de Seguridad

2018

Política de Gobierno Digital.

Establece la seguridad digital como habilitador transversal de la política

2019

Política de Defensa y Seguridad

2020

Documento CONPES 3995

Formulación de una política Pública sobre ciberseguridad

2021

Proyecto de decreto de Ley de seguridad digital

.

2

Amenazas

En las siguientes diapositivas veremos algunos tipos de malware y definiciones

Errores de percepción

"Mi computador no contiene nada que le pueda interesar a nadie"

"Yo solo uso el computador para navegar, no para el trabajo"

"Yo no recibo emails ni chateo con nadie".

- Todos los **activos** son **igualmente importantes**.
- No existe un sistema **100% protegido**
- El recurso más valioso es la **información**
- Los Hackers **NO** son el mayor riesgo

¿Qué es el malware?

Malware procede del inglés **malicious software**, y es cualquier software que tiene como objetivo **infiltrarse en o dañar un computador** sin conocimiento de su dueño y con finalidades muy diversas

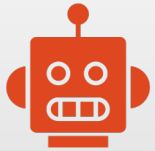
En el **lenguaje cotidiano** se utiliza la expresión **"virus informático"** para describir todos los tipos de malware

Tipos de malware

RANSOMWARE

Malware capaz de secuestrar nuestro dispositivo mediante el cifrado de los archivos principalmente.

Se solicita un secuestro para volver a la actividad normal.



BOTS

Son programas que a través de órdenes enviadas desde otra computadora controlan el equipo personal de la víctima, es decir convirtiéndola en un "Zombi".

Forman redes de ordenadores "Zombis" llamadas BotNets.

TROYANO (CABALLO DE TROYA)

Un programa caballo de Troya es una pieza de software dañino disfrazado de software legítimo.

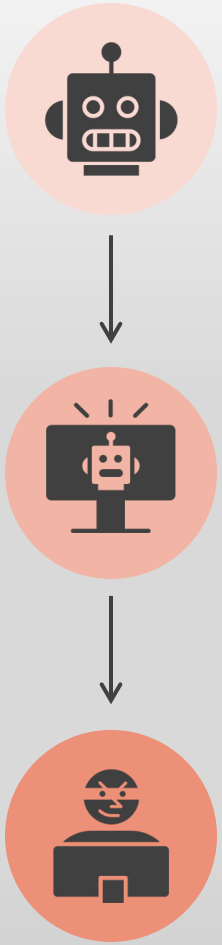
Los caballos de Troya no son capaces de replicarse por sí mismos y pueden ser adjuntados con cualquier tipo de software.

GUSANO (WORM)

Son similares a los virus, pero no dependen de archivos portadores para poder contaminar otros sistemas.

Pueden modificar el sistema operativo con el fin de auto ejecutarse como parte del proceso de inicialización del sistema.

¿Qué son las botnets?



Un **bot** es un código malicioso que se **instala en el sistema sin conocimiento del usuario** y que pasa inadvertido para éste actuando de forma silenciosa (combina características de troyano y rootkit).

Un **equipo infectado** por un bot pasa a estar dentro de la botnet o red de zombis, **red de ordenadores controlados** de modo remoto por un **hacker**.

El computador funciona con aparente normalidad pero el **hacker que controla esa botnet puede utilizarla para un uso fraudulento o delictivo**

La información es un recurso, como el resto de los activos comerciales importantes, tiene valor para una organización, y por consiguiente, debe ser debidamente protegida

Ministerios de Tecnologías de la Información y las Comunicaciones (MINTIC)
-Colombia-

¡Gracias!

conose
RED DE CONOCIMIENTO SOBRE SEGURIDAD CIUDADANA